UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/877,210	06/11/2001	Joji Onishi	109748	9564

25944 7590 02/07/2005

OLIFF & BERRIDGE, PLC
P.O. BOX 19928
ALEXANDRIA, VA 22320

EXAMINER	
QIN, YIXING	
ART UNIT	**PAPER NUMBER**
2622	

DATE MAILED: 02/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/877,210	ONISHI ET AL.	
	Examiner	Art Unit	
	Yixing Qin	2622	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 June 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 June 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *31 October 2001*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

I. Claim 1 and 7 are rejected under 35 U.S.C. 102(e) as being anticipated by DeBry (U.S. Patent No. 6,314,521).

The DeBry reference discloses the authorization of a printer to print a user requested document and the use of digital certificates to do so.

1. **Claim 1.**

A print data management apparatus for registering, in response to a data registration request which includes print data, the print data and for providing, in response to a data usage request, the print data relating to the data usage request, comprising:

- **a storage device that performs registration of the print data;**
- DeBry discloses in column 8, lines 39-41 that "[t]he database 40 is located in a secure server which also acts as a digital certificate authority 50, i.e., capable of issuing and validating digital certificates."

- In column 6, lines 33-67, DeBry describes the process in which a printer can obtain a requested digital certificate. In particular, in line 36 discloses that the printer sends a message (**"print data"**) to the server. Lines 40-42 discloses that this data contains model and serial numbers as well as an IP address. One would understand that the message would be stored in the database or the server, which is a computer, would inherently have some form of storage (RAM, hard disk, etc.) to, at least temporarily, store the incoming message in order to perform the steps needed for providing the printer with a digital certificate.
- **a registration device that registers the print data in said storage device; and**
- DeBry discloses in column 6, lines 52-53 that "...the server builds a digital certificate for the printer, registering itself as the certificate authority. The server then encrypts the content of the digital certificate with the certificate authority's private key, and sends it to the printer." One would understand that the registration is performed on the incoming message (**"print data"**) from the printer.
- **a providing device that provides the print data in said storage device;**
- The specification of the application explains in paragraph 16 of page 4 that "[f]or example, any providing device can be used as long as it directly or indirectly transmits the print data to a user or a print terminal." This indicates that the providing device could be any cables or buses in or connected to the server since they are the means by which data would be transferred from the storage

means to another location (such as a CPU for processing the data, or to a network location).

- Networked devices would inherently contain some for of communication that provides data to various networked locations from a server or a printer (i.e. using a network cable, or using a wireless connection). Devices such as the server computer or the printer in the DeBry reference would inherently contain internal cables or buses for communication and data transfer purposes.
- **such that, when the data registration request is received, said registration device registers the print data included in the received data registration request in said storage device, in association with authentication information for authenticating whether or not a user is eligible to use the print data, and said registration device transmits usage certificate data which includes the authentication information; and**
- DeBry discloses in column 6, lines 52-57 that "...the server builds a digital certificate for the printer, registering itself as the certificate authority. The server then encrypts the content of the digital certificate with the certificate authority's private key, and sends it to the printer. Since the digital certificate is encrypted, it is safe to transmit."
- Even though the DeBry reference focuses primarily on disclosing the encryption of a message sent by a printer, it also discloses in column 8 lines 45-50 that an administrator tells the printer to obtain a digital certificate. DeBry explains the reasons for letting a printer obtain a certificate in his description of prior art in the

background in column 4, lines 40-67 and column 5, lines 1-20. Basically, a user may not wish to download or store the documents to be printed in his/her own terminal due to storage and/or security issues. Thus, the printer would need to have the same access privileges as the user in order to print the user's documents. One would understand that the allowing of the printer to have access privileges indicates that the user (or administrator) using it has the privileges as well.

- **when the data usage request which includes the authentication information is received, and when the authentication information in said storage device that corresponds to the print data relating to the received data usage request and the authentication information included in the received data usage request satisfy a predetermined relationship, said providing device transmits the print data in said storage device relating to the received data usage request.**
- The DeBry reference disclose in column 8, lines 65-67 and column 9, lines 1-10 how a certificate authority 50, can verify the printer's identity using the incoming message generated by the printer. In particular, column 9, lines 2-10 describes all the various matches needed to verify the printer's identity. The verification of the various fields shows that there is verification of a "**predetermined relationship**" since the certificate authority looks up information in the database to compare to the incoming message.

- Column 9, lines 15-23 discloses the generation of a public/private key for the printer. Lines 21-23 discloses that "[t]he new private key, along with the digital certificate, is encrypted using the printer's hardware encryption key and sent to the printer."

7. **Claim 7**

A computer-readable storage medium having stored therein a print data management program to be applied to the print data management apparatus as set forth in Claim 1, comprising:

- **a program for causing a computer to perform processing implemented by the registration device that registers print data in the storage device and processing implemented by the providing device that provides the print data in said storage device;**
- **such that, when a data registration request is received, said registration device registers the print data included in the received data registration request in said storage device, in association with authentication information that authenticates whether or not a user is eligible to use the print data, and said registration device transmits usage certificate data which includes the authentication information; and**
- **when a data usage request which includes the authentication information is received, and when the authentication information in said storage device which corresponds to the print data relating to the received data usage**

request and the authentication information included in the received data usage request satisfy a predetermined relationship, said providing device transmits the print data in said storage device relating to the received data usage request.

- The above limitations have been addressed by the rejection to claim 1. In this case, there happens to be a program that takes care of all of these functions. However, the DeBry reference discloses in column 9, lines 59-63 that his "... invention may be implemented as a machine, process, or article of manufacture by using standard programming and/or engineering techniques to produce programming software, firmware, hardware, or any combination thereof." Column 9, lines 64-67 and column 10, lines 1-7 discloses that the program could be stored in computer-usable media.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

II. Claims 3-5 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeBry (U.S. Patent No. 6,314,521).

3. **Claim 3**

The print data management apparatus according to claim 1,

- **the usage certificate data further including a network address that uniquely specifies the location of the apparatus on a network to which the apparatus is connected.**
- DeBry discloses in column 6, lines 37-39 that "...the printer sends a two-part message to the server. The first part of the message contains the printer model and serial number, the printer's network address (e.g., IP address), and a request for a digital certificate." Although this specifies the IP address of the printer and not of the server, which contains the database, (**"data management apparatus**"), it would have been obvious to one of ordinary skill in the art to include an IP address in the certificate. The motivation would be to identify the location from where the certificate would be coming from. This information should be apparent to the user/printer since it has to know the location of the server in order to send messages to it. The usage of IP/network address to identify components on a network is well-known.

4. **Claim 4**

The print data management apparatus according to claim 1,

- **the usage certificate data further including a network address that uniquely specifies, on a network, the storage location of a program that transmits**

the data usage request which includes the authentication information to the apparatus, the program being stored in the network.

- Again, as mentioned above in the rejection to claim 3, the message sent from the printer contains an IP address as a form of identification. Although this specifies the IP address of the printer and not of location of storage of the program that transmits data usage requests, it would have been obvious to one of ordinary skill in the art to include an IP address in the certificate. The motivation would be to identify the location from where the data usage requests would be coming from.
- This information should be apparent since components on a network need to know the address of other components so that they can communicate. The usage of IP/network address to identify components on a network is well-known. It would simply be a matter of design to include this information in data being transferred.

5. Claim 5

The print data management apparatus according to claim 1,

- **when a network address is included in the data registration request, said registration device transmitting the usage certificate data to a destination specified by the network address, and, when no network address is included in the data registration request, said registration device**

transmitting the usage certificate data to the sender of the data registration request.

- As discussed above, in the rejection to claim 3, the message from the printer that requests a digital certificate includes the IP address of the printer. Column 9, lines 15-23 discloses the generation of a public/private key for the printer. Lines 21-23 discloses that "[t]he new private key, along with the digital certificate, is encrypted using the printer's hardware encryption key and sent to the printer." The IP address in the message sent from the printer would identify where the printer was.
- DeBry discloses in column 9, lines 6-9 that "[t]he certificate authority 50 then checks to see if the IP address...found in the encrypted part of the message matches the IP address the message was sent from." This indicates that the certificate authority knows where the message is coming from. Even if no IP address was specified, it would have been obvious to one of ordinary skill that e printer requesting a certificate would be the one that the server should sent the certificate back to.

III. Claims 2, 6 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeBry (U.S. Patent No. 6,314,521) in view of DeBry (U.S. Patent No. 6,385,728). This second DeBry reference will henceforth be referred to as DeBry2.

The second DeBry reference, Debry2, also discloses information regarding the authentication of a printer to print private documents. It, however, provides more details about how the user can obtain "will-call" certificates that allow him/her to tell a print server to print a particular file. This is done using digital certificates as well, which provides authentication of the user as well as the user's request.

2. **Claim 2**

The print data management apparatus according to claim 1, wherein:

- **said registration device registering the print data included in the received data registration request in said storage means, in association with usage count information which indicates the number of times the print data is permitted to be used;**
- **and when a usage count in the usage count information in said storage device which corresponds to the print data relating to the received data usage request is greater than or equal to a predetermined number, said providing means transmits the print data in said storage means relating to the received data usage request to a print terminal, and, when the usage count in the usage count information is less than the predetermined number, transmission of the print data is prohibited.**
- The DeBry reference does not explicitly disclose the use of a count for determining whether print data is allowed to be printed. However, it does disclose in Fig. 1 (item 15) a validity period (column 9, line 20). One can see

from the description in Fig. 1 that the validity period of the digital certificate is only usable for a period of time. The goals is to prevent printers (or rather the users using them) to have access forever. This is much like the idea of the using a usage count, where data can only be accessed so many times. Both the date range and the count set thresholds on the accessing of data.

- The secondary reference, DeBry2, discloses in column 10 lines 30-37 that "[i]t is assumed that in the emerging world of electronic commerce, publishers will often want to sell the rights for only one printed copy, just as they would sell one copy of a printed book or journal. Allowing the printable version of the document to exist in the clear (i.e. without any encryption) anywhere within the system places the publisher at risk, since illicit copies could be made and printed multiple times." This one copy would be a **usage count** of copies that can be printed with a particular authentication (see column 10, lines 45-62 for further explanation.)
- One can store this value of one copy in a field much like the way the validity period is stored in the first DeBry reference. One would understand that the publisher has to set this count to one for a digital certificate for a request to print a copy of a book or journal.
- The requesting of printing copies of a document is well-known (i.e. a user can request 5 copies of a document be printed simply by setting a number of copies field to 5 in a print execution program). Although the example given by DeBry2 shows that a user only requests one copy of the document (also see Fig. 5 of DeBry), one would understand that there would be a denial of service if a user

requested more than one document. (i.e. an **usage count** of one copy is less than **predetermined number** of five copies that user requested).

- Since both references are in the art of securely printing documents and authentication, it would have been obvious to one of ordinary skill in the art at the time of the invention to have improved the invention in the first DeBry reference with a count (or counter) of the number of copies a private or secure document is to be printed. The motivation would be to expand the capabilities of the first DeBry invention by allowing it to limit not only the amount of time a digital certificate was accepted for, but also the number of copies that can be used to print using the digital certificate.

6. **Claim 6**

The print data management apparatus according to claim 1,

- **when a network address is included in the data usage request, said providing device transmitting the print data to a destination specified by the network address, and, when no network address is included in the data usage request, said providing device transmitting the print data to the sender of the data usage request.**
- Again, the message from the printer contains the IP address of the printer. However, the DeBry only discloses that the private key and the digital certificate is returned to the printer (column 9, lines 21-23). There is no mention of the returning of the print data to the printer. However, the secondary reference,

DeBry2, discloses in column 7, lines 15-42 a brief explanation of a "will-call certificate" that is created and given to a user, which allows a print server access to private information or documents to be printers. In particular, lines 20-25 discloses that "[t]he will-call certificate 40 (FIG. 2) contains the following fields: distinguished name of the document source 41, which tells the print server exactly where to go to get the document (e.g., including the Internet address); the path to the document file 42 to find the document within the file system; and the digital signature of the provider of the document 43."

- Since both references are in the art of securely printing documents and authentication, it would have been obvious to one of ordinary skill in the art at the time of the invention to request and return data containing information about a specific document to be printed. The motivation would be to expand the capabilities of the first DeBry invention by allowing that printer not only to authenticate itself to a server, but also to obtain documents from that server to be printed.

8. **Claim 8**

A computer-readable storage medium having stored therein usage certificate data to be transmitted by the print data management apparatus as set forth in Claim 1, comprising:

- **a program for storing authentication information that authenticates, by said print data management apparatus, whether or not a user is eligible to use**

the print data and a network address that uniquely specifies, on a network, the storage location of a program for transmitting a data usage request that includes the authentication information to said print data management apparatus, the program being stored in the network.

- Although the first DeBry reference discloses whether a printer is eligible to print certain information, it does not go into detail about the involvement of the user and what the user can do with a returned verified/certified information from a certifying source.
- As explained in claim 6 above, Debry2 discloses a will-call certificate that includes an Internet address telling the print server where to access a file to be printed. Column 7, lines 47-49 discloses that "[t]he print request specifies which document is being requested, and where the document is. The request also contains the "will-call" certificate which gives the printer the credentials to go to the document source to get the document." Since the will-call certificate is digitally signed (Fig. 2, item 43) and may contain a password (column 7, line 39-41), one would understand that it would be used to determine whether a user was eligible to use print data (i.e. print a private file).
- Since both references by DeBry are in the art of authentication, it would have been obvious to one of ordinary skill in the art at the time of the invention to further the first DeBry invention by including the capability to give the user the ability to specify a print server to securely print a private document. The

motivation would be to allow users the ability to choose where a private document is to be printed.

- As with the first DeBry reference, Debry2 discloses that his invention may be implemented as a combination of hardware and/or software. (column 11, lines 16-62 expands on the various forms that the invention could take on)

IV. Claims 9 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over DeBry (U.S. Patent No. 6,385,728).

9. Claim 9

A method of using print data by a computer system, comprising:

- **providing print data with a provider, including registering the print data in a storage device in association with authentication information that authenticates whether or not a user is eligible to use the print data; and transmitting usage certificate information that includes the authentication information to the user of the print data;**
- DeBry2 discloses in column 7, lines 20-25 discloses that "[t]he will-call certificate 40 (FIG. 2) contains the following fields: distinguished name of the document source 41, which tells the print server exactly where to go to get the document (e.g., including the Internet address); the path to the document file 42 to find the document within the file system; and the digital signature of the provider of the

document 43." The will call certificate is created in the document source 10 (column 7, lines 15-17, which can be a server (column 8, line 43). It contains various authentication information (such as a key – column 7, line 28 – and/or a password – column 7, line 40). The server would inherently have some database or some other form of storage (RAM, hard disk, etc.) to store the will call certificate, which contains authentication information. One would understand that this will call certificate verifies whether or not a user is able to print a certain document.

- Although the will call certificate will register where to get the print data (such as a document) it does not record the print data itself. However, since the server knows where to get the data, it could simply go and obtain this print data if it is deemed necessary to do so. The motivation would be to allow users to preview data or have a local copy of the data.
- DeBry2 discloses in column 7, lines 15-19, that "...the document source 10...will give the requesting user a will-call certificate..." (i.e. "**transmit the certification information to a user.**")
- **with a user, receiving the usage certificate data; and transmitting a data usage request which includes the authentication information; and**
- Debry2 discloses in column 7, lines 43-45 that "...the user 20 takes the "will-call" certificate, builds a print request, and sends the print request, via communication 3, to the print server."

- **the providing step further including receiving the data usage request; and transmitting the print data in said storage device relating to the received data usage request and the authentication information included in the received data usage request satisfy a predetermined relationship.**
- DeBry2 discloses in column 7, liens 50-55 that "[t]he print server 30 goes to the document source 10, requests the document, via communication 4, and gives the document source the will-call certificate which verifies that the printer is allowed to get that document. The print server also gives the document source a server certificate, or digital certificate." This shows that the document source receives a request for using the data (i.e. to print a document).
- DeBry2 further discloses in column 8, lines 32-36 that "[a]fter verifying that the printer is who the printer purports to be, and verifying that the will-call certificate is unchanged from the one issued by the document source, then the document source can securely send the document to the printer, via communication 5." Column 10, lines 6-31 discusses various checks the document source performs to verify the digital signatures used by the printer/print server.

10. Claim 10

The method of using print data according to Claim 9,

- **the providing step further including registering the print data in said storage device in association with usage count information that indicates the number of times the print data is permitted to be used; and**

transmitting, when a usage count in the usage count information in said storage device that corresponds to the print data relating to the received data usage request is greater than or equal to a predetermined number, the print data in said storage device that corresponds to the received data usage request to a print terminal, and prohibiting transmission of the print data when the usage count in said usage count information is less than the predetermined number.

- This claim essentially the same as claim 2 above. As mentioned in the rejection to claim 2, DeBry2 disclosed the printing of one copy of a printed book or journal. The explanation given by the examiner above explains why it would be obvious for the DeBry2 invention to have some sort of determining mechanism or program for determining whether a user would be allowed to print a document (such as a book or journal) even though the DeBry2 reference does not explicitly disclose what happens when an user requests more than one copy of a document to be printed.
- This allows a print/file server to permit an user to or prevent a user from printing multiple copies of a document. The motivation would be to allow an user to print what is rightfully requested by an user (i.e. user only paid for one copy of a document, so he/her should not be able to print five copies.)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Yixing Qin whose telephone number is 703-306-4142. The examiner can normally be reached on M-F 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Edward Coles can be reached on 703-305-4712. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

YQ